IT Unit 4

Topic 2

**Ch 6, Security Measures** (Informatics, p 275-280)

Threats to data and information

1. Why is it important to maintain security over an organisation’s data & information? Explain the consequences of failing to maintain security.

It is important to maintain security over an organisation’s data and information as it can be damaged, destroyed, stolen, copied or deleted in many of ways, majority of these being avoidable.

1. Accidental threats:
   1. List causes of accidental threats with examples

User Error: deleting vital records or files, damaging databases, damaging hardware, inviting unauthorised person into secure areas and choosing weak passwords.

Poorly Managed Backups: having infrequent backups, inadequate storage media and a lack of testing of the backup regimen

Poor Management: Staff who are dismissed may delete files or steal data before leaving, disgruntled IT manager leaving without telling the network administrator password causing the company to be locked out of their own system, staff being untrained in cases of emergency and security updates not being installed.

Loss of Data Storage Devices: USB devices are left plugged into public computers, portable hard disks or laptops being lost and obsolete computers being sold without first being reformatted.

Unsafe Internet Usage: Malware via Trojans accessing computer via internet and employees opening infected email attachment, reply to spam, respond to phishing attempts, click links in suspicious emails or mistakenly send valuable information to the wrong email.

* 1. How can each of these threats be prevented or rectified?

User Error: Train staff thoroughly in the use of software, computers and company procedures, such as filing naming conventions, and how to use strong passwords and recognise social engineering.

Poorly Managed Backups: Ideally, organisations should backup all their data every day and store their backups offsite. They should also test their backup procedures to ensure they are working properly and backups can be restored.

Poor Management: revoke network access of employees before they are fired, keep a secret master password [unknown to everyone other than the employer] that gives complete access to the digital system, use copy-restricted keys or electronic security passes that cannot be copied, carry out drills to practice all aspects of the disaster recovery plan, use network monitoring software to detect intrusions and to log all network activity and enforce policies forbidding the use of unauthorised equipment.

Loss of Data Storage Devices: encrypt all portable storage devices and laptops and reformat or destroy the hard disks of obsolete computers.

Unsafe internet Usage: Use the networks proxy server to block all access to all internet sites apart from those needed by staff to do their work, ensure malware scanners are running and are up-to-date.

1. Technical threats:
   1. List causes of technical threats with examples.

Equipment Failure: failure of servers, hard disks or core communications equipment can cause loss of access to network data, data loss and loss of productivity and computers in humid, hot or dusty conditions tend to fail quickly.

Electric Problems: Blackouts, brownouts, spikes and power surges can damage sensitive electronic equipment.

Software Bugs: Bugs in an operating system, device driver or application can crash and lose data, or make computers vulnerable to attack

Improperly Configured Equipment: Dangerous security holes or poor performance can be caused by equipment that has been configured incorrectly.

Malware Infection: Once a malware enters a system, it can spread and expose an entire network to exploitation and data loss.

* 1. How can each of these threats be prevented or rectified?

Equipment Failures: Do not buy cheap or underpowered equipment, maintain and update hardware properly and handle equipment carefully and house servers in secure, air-conditioned environments.

Electric Problems: Servers need battery-backed uninterruptible power supplied [UPS]

Software Bugs: Regularly update software and operating systems

Improperly Configured Equipment: Read the manual. Visit manufacturer forums to learn of problems and cures from other product users.

Malware Infection: Use vulnerability management software to perform automated scans of systems to discover security weaknesses such as open ports, unpatched software and SQL injection vulnerability.

1. Deliberate threats:
   1. List causes of deliberate threats with examples.

Malicious Staff: It is estimated that 18% of deliberate attacks on systems come from staff within an organisation.

Crackers: Crackers [Malicious Hackers] may penetrate systems to plant botnet software or keyloggers so they can control system remotely to steal data, discover passwords or banding information, conduct DDoS [distributed denial of service] attacks or turn computers into zombies that deliver spam.

Identity Theft: Once enough personal information is known about victims; their bank accounts can be raised or their credit misused.

Equipment Thieves: thieves may walk off with expensive hardware, along with the irreplaceable data stored on it.

Vandals: People may physically damage equipment or electronically deface a website for fun, revenge, fame, money or a challenge.

Espionage: Political espionage aims to discover state secrets of a rival nation and corporate espionage aims to learn about a competitor’s new product, business plans, or how much they plan to bid on a government tender.

Fraudsters: Scammers, phishers, and social engineers manipulate gullible staff to gain unauthorised information or payment by trickery.

* 1. How can each of these threats be prevented or rectified?

Malicious Staff: Hire external consultants to conduct security audits and examine networks for secret ‘back door’ entrances so employees cannot enter the system after leaving the company, booby traps that damage the system if employees are aggrieved and unauthorised network privileges, such as staff giving themselves administrator access.

Crackers: Constantly run malware scanners. Run network monitoring software to identify attempts to break in.

Identity Theft: No dot reuse passwords on different sites. Keep malware scanners up to date. Avoid suspicious sites. Browse in ‘incognito’ mode. Carefully check software installations for devious extra software additions. Use multi-factor authentication whenever it is offered.

Equipment Thieves: Improve physical security and strengthen security procedures. Record serial numbers of equipment so police can identify stolen equipment. Encrypt hard disks.

Vandals: Improve physical and electronic security. Keep your files backed up.

Fraudsters: Train staff to recognise deceptive practices.

1. Event-based threats:
   1. List causes of event-based threats with examples.

Natural Disasters: Disasters such as fires, floods, storms, lightning and earthquakes can cause equipment failures and even destruction.

Manmade Disasters: Acts or war, riots, terrorism or civil unrest can cause devastating disruptions to information systems.

* 1. How can each of these threats be prevented or rectified?

Natural Disasters: Conduct backups, ensuring that all backups are kept offsite. Maintain and practice your data disaster recovery plan. Consider storing data in buildings designed to withstand earthquakes or that are elevated above flood plains.

Manmade Disasters: Monitor the news. With enough early warning, data managers may have enough time to protect data.